ROUTING AND RECORD SHEET

SUBJECT: (Optional) Security Requirements for Agency Classified Automated Information Systems Procured Beginning in FY-88

DDA SUBJECT FILE COPY

FROM: STAT [redacted]
Director of Security
STAT [redacted]

EXTENSION

NO.

DATE 4 MAR 1987

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS
1. DDA\EXA 7D-24 Hdqs.	5 MAR 1987	3/5	
2. ADDA			
3. DDA	6 MAR 1987		
4.			
5.			
6. D/OS			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

A new step toward standards – this time in ADP security. The problem, as with all standards, is audit and enforcement. We ought to be sure OS/ISSD is up to this much work.

STAT [redacted]

Would assume an OIT Chop? [illegible]

3 to 6: Proceed. Get the draft on the table and circulating.

10-13

STAT [redacted]

~~SECRET~~

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030017-3

MEMORANDUM FOR: Deputy Director for Administration

STAT FROM: [redacted]
Director of Security

SUBJECT: Security Requirements for Agency Classified Automated Information Systems Procured Beginning in FY-88

1. This memorandum is to alert you to an Office of Security (OS) initiative in informtion systems security. I believe it is desirable to establish by regulation an Agency standard concerning minimum security requirements for classified multi-user Automated Information Systems (AIS) procured after the end of FY-1987. Such a regulation would help ensure that security requirements are included in long range planning for the procurement or modification of AIS by the diverse procurement and system development elements which exist in CIA. [redacted] STAT

2. As you are aware, the National Security Agency/National Computer Security Center (NSA/NCSC) has established technical security requirements (the Department of Defense Trusted Computer System Evaluation Criteria, commonly known as the "Orange Book") for computer vendors to incorporate into their AIS. From your participation as the Agency's NTISSC representative, you are also aware of the current proposal to promulgate an NTISSC Policy in Controlled Access Protection (see attached). This policy references the Orange Book and includes the attributes of the minimum acceptable level of protection described therein. Information Systems Security Division (OS/ISSD) is currently drafting for coordination among concerned components a proposed Headquarters Notice which would implement an Agency version of the Orange Book. [redacted] STAT

3. The minimum acceptable level of "Controlled Access Protection" as specified in the Orange Book is Class C2. Systems in this class provide individual user accountability, file access control, and auditing of security-relevant events. Some AIS processing various types of sensitive data, e.g., Sensitive Compartmented Information, should be afforded levels of security higher than C2. Standards for these higher

STAT [redacted]

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030017-3

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030017-3

level systems (B1 and B2) are also specified in the Orange Book. Unfortunately, AIS meeting these standards are not widely available on the current market and it is not practicable to upgrade existing Agency systems. The C2 requirements can significantly improve AIS security and can easily be met by all vendors servicing this Agency. [redacted] STAT

4. By establishing a C2 system security requirement as a minimum, with B-level systems as a future goal, Agency procurement, security, and systems development elements will be able to: 1) evaluate and, as necessary, modify existing or near-term future AIS against a relatively fixed set of criteria and, 2) plan longer-term system development and procurement against the desirable B-level standards. The regulation would set guidelines for but not arbitrarily impose new standards on existing systems. It would require any proposed new systems or modifications to systems to be made in accordance with a security plan which incorporates C2 standards. [redacted] STAT

STAT [redacted]

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030017-3